

A SOLUTION TO SECURELY AND EASILY CONNECT EMPLOYEE-OWNED DEVICES IN THE ENTERPRISE

Over 45 million iPhones and iPads were sold in 2010*, most of them to consumers. These feature-rich smart devices with social networking, integrated cameras and high-speed Wi-Fi allow users to communicate and collaborate in ways unimagined just a few years ago. Consumers are now accustomed to the productivity enhancements these mobile devices bring to their lives and are seeking to bring their personal experience into the workplace.

CIOs worldwide are contemplating adopting these mobile devices in the workplace, but a clear plan on what policies must be put in place to safeguard network services and company data must be developed to maintain a happy balance between enterprise needs and user demands.

These mobile devices are creating a new set of security, configuration and management challenges for IT departments. Since these devices may have security vulnerabilities that do not apply to IT-supplied PCs with locked-down configurations, IT groups are unsure of the implications of endorsing the use of these new, unmanaged and potentially insecure mobile devices.

Most networks today allow any device onto the network if user presents a valid username and password combination. The underlying assumption is that the device is trusted and only the user needs to be authenticated.

But with the shifting trend of untrusted employee-owned mobile devices requesting network access, it is critical to authenticate and authorize the user as well as the device itself. Once IT is able to distinguish between a user on an IT-supplied PC from a user on a personal iPad, network policies can be adapted for any device type.

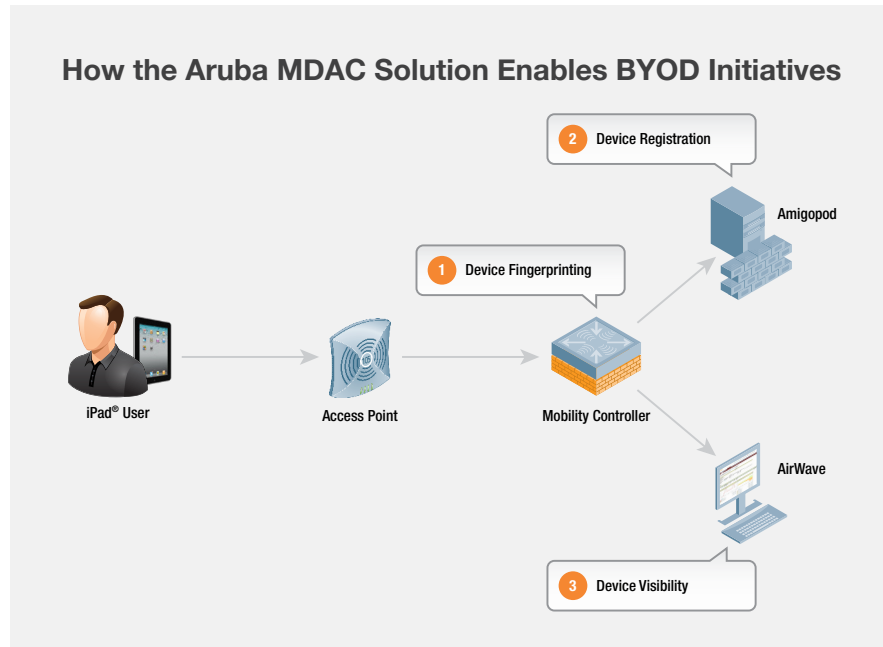
In order to enable employee-owned devices on the corporate network, the following IT concerns must be addressed:

- Secure enterprise data from unauthorized users and devices. Once employees have access to the corporate infrastructure using personal mobile devices, sensitive corporate data is available to anyone with access to that device. IT must have the ability to monitor the mobile device and apply access policies to restrict unauthorized access.
- Provide reliable services to a growing number of mobile users. Employees expect to take full advantage of the multimedia capabilities of their personal mobile devices. These users expect the network to be available and provide reliable services for mobility applications.
- Keep IT budgets manageable while rolling out new mobility initiatives. While IT has been well prepared to support one device per employee, the mobile device explosion has armed every employee with at least one additional device like an iPhone or an iPad, in addition to the corporate laptop or desktop. Enabling multiple devices per employee increases the demand on the helpdesk staff, network infrastructure and network services like DHCP and security.

The Aruba Networks[®] Mobile Device Access Control (MDAC) solution addresses these IT concerns and more. MDAC provides a clientless mechanism to identify, provision, secure and manage employee-owned devices while minimizing IT overhead and simplifying operations.

The Aruba advantage

- **Seamless device provisioning.** Automatically configure, authorize and provision Apple mobile devices with secure authentication policies.
- **Secure enterprise-grade connectivity.** Control a mobile device's access to corporate data, ensuring content security and reducing risk against lost devices.
- **Superior quality of service (QoS).** Dynamically identify multimedia applications such as multicast video, Apple FaceTime and SIP voice over IP for uninterrupted always-on service.
- **Device-centric centralized management.** Control total bandwidth usage per user or device, easily scale to support increased number of IP address assignments and enable centralized Apple device inventory management.



The Aruba MDAC solution is comprised of three distinct capabilities:

1. The first is device fingerprinting, which is built into ArubaOS™ for Aruba Mobility Controllers and accurately identifies device type – whether it’s an iPhone or iPad or even a laptop running Windows or Mac OS. With device fingerprinting, IT can enforce global policies like no iPads on the corporate network or even restrict bandwidth for iPhone applications. Device fingerprinting by itself will meet most requirements by providing full access control and policy management for all mobile devices.
2. The second is the Aruba Amigopod™ access management system, which automates device configuration and user enrollment through an easy-to-use self-service configuration portal. This web portal allows users to self-configure their Apple iOS devices and prime them for the network with no IT involvement. Aruba Amigopod is only needed by organizations that intend to go the extra step to configure and manage employee-owned devices or roll out corporate owned iOS devices with ease.
3. The third is the Aruba AirWave® multivendor wired and wireless management system. AirWave provides a centralized view of the network and enables device-specific monitoring, troubleshooting and reporting across multiple locations. With AirWave, IT can monitor trends like which devices are most common on the network or get a report showing how much bandwidth is being consumed by these devices.

The Aruba MDAC solution helps IT organizations lay the groundwork with comprehensive management and control over employee-owned mobile devices, enabling workers to stay productive by securely connecting to corporate resources using any device, no matter where they happen to be.

The Aruba MDAC solution is also complimentary to Mobile Device Management (MDM) solutions. MDAC provides security for the network and enforces network-use policies for the devices while MDM focuses solely on device configuration.

* Apple Fiscal 2010 10-K Filing



WWW.ARUBANETWORKS.COM | 1344 Crossman Avenue. Sunnyvale, CA 94089

1-866-55-ARUBA | Tel. +1 408.227.4500 | Fax. +1 408.227.4550 | info@arubanetworks.com